UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**CRIMINAL COMPLAINT**
	:	
v.	:	Honorable James B. Clark, III
	:	
ROSTISLAV PANEV	:	Mag. No. 24-12254
	:	
	:	**FILED UNDER SEAL**

I, Andrew Feiter, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

s/*Andrew Feiter*
Andrew Feiter
Special Agent
Federal Bureau of Investigation
Special Agent Andrew Feiter attested to this Affidavit by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to before me telephonically
on August 9, 2024

Honorable James B. Clark, III
United States Magistrate Judge

Signature of Judicial Officer

ATTACHMENT A

COUNT 1
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers – 18 U.S.C. § 371)

From at least as early as in or around January 2022 through at least as recently as in or around February 2024, in the District of New Jersey and elsewhere, the defendant,

ROSTISLAV PANEV,

did knowingly and intentionally conspire and agree with others to commit offenses against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to persons during a one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and cause damage affecting 10 or more protected computers during a one-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), and (c)(4)(B)(i); and

b. to knowingly and with intent to extort from any person any money and thing of value, transmit in interstate and foreign commerce any communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to Title 18, United States Code, Section 1030(a)(7)(B), (a)(7)(C), and (c)(3)(A).

In violation of Title 18, United States Code, Section 371.

COUNT 2
(Conspiracy to Commit Wire Fraud – 18 U.S.C. § 1349)

From at least as early as in or around January 2022 through at least as recently as in or around February 2024, in the District of New Jersey and elsewhere, the defendant,

ROSTISLAV PANEV,

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Andrew Feiter, am a Special Agent with the Federal Bureau of Investigation (the "FBI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and photographs of the evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Overview

1. Law enforcement is investigating the LockBit ransomware group, which, since it first appeared in or around January 2020, has ranked among the most prolific and destructive ransomware groups in the world. That investigation has established that the defendant, ROSTISLAV PANEV, has provided coding and development services to the LockBit ransomware group since at least as early as in or around January 2022 and has received at least as much as approximately $230,000 in cryptocurrency transfers from the LockBit group during that time.

Background on the LockBit Ransomware Group and Related Technical Matters

2. At times relevant to this Complaint:

a. Ransomware was a type of malware used by cybercriminals to encrypt data stored on a victim's computer system, leaving that data inaccessible to and unusable by the victim, and to transmit data stored on a victim system to a remote computer, or both. Following a ransomware attack, perpetrators typically demanded a ransom payment from their victims, threatening to either leave encrypted data unusable, to publish or sell stolen data if the demanded ransom was not paid, or both.

b. "LockBit" was a ransomware variant that first appeared at least as early as in or around January 2020. Between then and the present, members of the LockBit conspiracy have executed at least around 2,500 LockBit attacks against victim systems both in the United States and in nearly 120 other countries around the world, including the United Kingdom, Israel, France, Australia, Germany, Argentina, Kenya, Switzerland, Finland, the Netherlands, Japan, Canada, Spain, Italy, and China. During that time, LockBit has extorted at least approximately $500 million in ransom payments and caused billions of dollars in further damage.

c. In many instances, LockBit perpetrators have posted highly confidential and sensitive data stolen from LockBit victims to a publicly available website under their ownership and control (the "LockBit Data Leak Site"), generally to punish victims who refused to pay a ransom. In this way, LockBit has at times constituted one of the most active and destructive ransomware variants in the world.

d. The FBI has been investigating the LockBit conspiracy since in or around March 2020.

e. The LockBit ransomware variant, like other ransomware variants, has operated through the "ransomware-as-a-service" model ("RaaS"). The RaaS model comprises two groups of ransomware perpetrators: developers and affiliates. The developers design the ransomware and then recruit affiliates to deploy it. The affiliates, in turn, identify vulnerable computer systems, unlawfully access those systems, and deploy on those systems the ransomware designed by the developers. When victims make ransom payments after successful ransomware attacks, the developers and the affiliates each take a share of those payments.

f. Based on my training, experience, and investigation, I believe that it is widely known—including to LockBit conspiracy members themselves—that the LockBit campaign employs the RaaS model and that the LockBit conspiracy comprises numerous affiliates all seeking to deploy LockBit on victim computer systems for profit.

g. In particular, this investigation has established through blockchain analysis[1] and other evidence that after a successful LockBit

---

[1] Many virtual currencies publicly record all of their transactions on what is known as a blockchain. A blockchain is essentially a distributed public ledger, run by a decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. Blockchains can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies. The Bitcoin blockchain is the most popular blockchain to date.

While the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (*e.g.*, the Bitcoin blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. In addition to using publicly available blockchain explorers, law

attack leading to a ransom payment, developers retain 20 percent of the ransom payment and affiliates retain the remaining 80 percent. This 80-20 split is clearly understood and accepted by all members of the LockBit conspiracy.

h. Moreover, and like other ransomware variants, this investigation has established that the LockBit variant relies on a "control panel" for its operation. In the ransomware context, a "control panel" is a software dashboard made available to an affiliate by the developers to both provide that affiliate with tools necessary for the deployment of ransomware attacks and to allow developers to monitor their affiliates' activities.

i. Among other things, the LockBit control panel includes a so-called "builder," or a feature that allows affiliates to develop custom builds of the LockBit ransomware payload for particular victims (*i.e.*, a customized platform for each affiliate/victim). The LockBit control panel also allows affiliates, among other things, to communicate with LockBit victims for ransom negotiation and to publish data stolen from LockBit victims to the LockBit Data Leak Site.

j. LockBit members, like other cybercriminals, frequently employed fraudulent techniques to gain and maintain unauthorized access to their victims' computer systems. One of these techniques was the use of "phishing," or the fraudulent practice of sending emails or other messages purporting to be from reputable sources in order to induce victims to reveal personal information, such as passwords and other access credentials. As another example, on or about November 21, 2021, a LockBit victim in Essex County, New Jersey sustained a LockBit attack facilitated by the deployment of malicious software on that victim's system disguised to appear like a standard Microsoft Windows system process.

k. Other LockBit victims within the District of New Jersey have included a municipal utilities operator in Gloucester County, New Jersey, which was attacked on or about November 9, 2022; a school district in Somerset County, New Jersey, which was attacked on or about June 13,

---

enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions and to identify groups of virtual currency addresses assessed to belong to the same individual or entity. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable. In particular, I refer in this Complaint to groups of virtual currency addresses assessed through these techniques to belong to the same individual or entity as a "cluster."

2023; and a healthcare provider in Union County, New Jersey, which was attacked on or about November 2, 2023.

l. Forum-1 was a forum hosted on the dark web known to law enforcement to be used by cybercriminals to communicate with each other, advertise criminal products and services, and recruit others to various cybercriminal ventures. Forum-1 allowed users to make publicly viewable posts on the forum, and also to exchange private messages with each other. Forum-1 also required users to pay a registration fee to join the forum, usually paid in cryptocurrency.

m. Service-1 was an end-to-end encrypted messaging platform.

n. Processor-1 was a payment processing service that allowed users to make payments for products and services.

Background on PANEV and Related Individuals

3. The defendant, ROSTISLAV PANEV ("PANEV"), is a dual Israeli and Russian national. As detailed below, this investigation has established that PANEV has participated in the LockBit group as a developer since at least as early as in or around January 2022. More specifically, this investigation has shown that PANEV has, since at least in or around January 2022, provided coding and development services to the LockBit group in support of LockBit infrastructure (e.g., the LockBit control panel) and has received at least as much as approximately $230,000 in Bitcoin for those services.

4. Dmitry Yuryevich Khoroshev ("Khoroshev") is a Russian national. Khoroshev was charged by an indictment unsealed in May 2024 for being the primary leader, developer, and administrator of the LockBit ransomware group since LockBit's inception. *See United States v. Dmitry Yuryevich Khoroshev*, 24-cr-299, D.E. 1 (the "Khoroshev Indictment").

5. Throughout the LockBit conspiracy, the monikers "LockBit" and "LockBitSupp" have been used to publicly promote and speak for LockBit, such as on cybercriminal forums and to media outlets. As alleged by the Khoroshev Indictment, Khoroshev himself was the owner and controller of these monikers at times relevant to the LockBit conspiracy.

6. In particular, and as is relevant to this Complaint, the moniker "LockBit" was used on Forum-1 to speak for the LockBit group on Forum-1 at relevant times—for example, to make announcements related to LockBit and to recruit new affiliates to the LockBit group. As with the other LockBit and LockBitSupp facilities, Khoroshev owned and controlled the LockBit moniker on Forum-1 at all relevant times.

PANEV Communicated with LockBit Regarding LockBit Infrastructure

7. Law enforcement has obtained evidence showing that PANEV communicated with Khoroshev regarding LockBit on Forum-1 using a certain Forum-1 moniker, "Moniker-1."

8. Specifically, law enforcement has obtained records of the Moniker-1 account on Forum-1. Those records show that Moniker-1 was registered on Forum 1 in or around November 2018. A review of publicly available Forum-1 posts also reveals that Moniker-1 has at various times posted advertisements and solicitations for cybercriminal services, including a solicitation for malware samples and an advertisement for a service allowing users to create their own "droppers," or malware that delivers other malware to a victim computer.

9. The Moniker-1 records also show that the following direct messages were exchanged between Forum-1 users "LockBit" and Moniker-1 in or around January-February 2022:

Approximate Date and Time	Forum-1 Sender	Message (translated from Russian)
1/31/2022 at 19:11	LockBit	Hello, where have you disappeared to?
2/1/2022 at 10:28	Moniker-1	Hello, I got really sick. It is better now. I will get in touch tomorrow.
2/2/2022 at 12:29	Moniker-1	I wrote into latest [Service-1]. It has been silence so far. If I will be needed, I am ready.
2/5/2022 at 14:39	LockBit	The builder in the panel needs to be finished urgently.

10. As explained above, in this context, "the panel" refers to the LockBit control panel maintained by the LockBit developers, and "the builder" refers to the control panel feature that generates custom builds of the LockBit malware payload for deployment by affiliates against victim computer systems. Thus, law enforcement assesses that this exchange evinces a discussion between the user of Moniker-1—whom, as explained below, this investigation has shown to be PANEV—and another LockBit developer—likely Khoroshev—regarding the development and maintenance of LockBit infrastructure.

11. Law enforcement has obtained evidence showing that PANEV owned and controlled the Moniker-1 account on Forum-1 at all relevant times.

PANEV Paid in Bitcoin to Register Moniker-1 on Forum-1

12. ***First,*** both the Forum-1 records and blockchain analysis show that the Forum-1 registration fee for Moniker-1—approximately 0.018 Bitcoin—was paid on or about November 16, 2018 from a particular cluster of Bitcoin addresses assessed by law enforcement, aided by blockchain analysis software, to be controlled by the same individual or entity. As explained below, law enforcement has obtained evidence showing that this cluster was owned and controlled by PANEV ("Cluster-PANEV-1").

13. Law enforcement has also identified a separate cluster of Bitcoin addresses assessed by law enforcement, aided by blockchain analysis software, to be controlled by the same individual or entity—and, like Cluster-PANEV-1, to be owned and controlled by PANEV ("Cluster-PANEV-2").

14. Law enforcement has obtained transaction records from "Processor-1," an electronic payment processor that accepts payments in Bitcoin. When users make Processor-1 transactions, they provide Processor-1 with information, including the user's name and email address. Processor-1 also records the Bitcoin address or addresses used to fund the transaction.

15. The Processor-1 records show that approximately 13 transactions were made through Processor-1 from Cluster-PANEV-1 and Cluster-PANEV-2 between in or around April 2018 and in or around January 2022, as shown below.

Approximate Date	User Email Address	Origination-Cluster	User Name
April 2018	Email-B	Cluster-PANEV-1	[none given]
October 2018	Email-A	Cluster-PANEV-1	q q
October 2018	Email-A	Cluster-PANEV-1	[none given]
November 2018	Email-A	Cluster-PANEV-1	[none given]
November 2018	Email-A	Cluster-PANEV-1	[none given]
January 2019	Email-A	Cluster-PANEV-1	q q
January 2019	Email-A	Cluster-PANEV-1	q q
January 2019	Email-A	Cluster-PANEV-1	q q
March 2019	Email-A	Cluster-PANEV-1	q q
July 2019	Email-A	Cluster-PANEV-1	q q

July 2019	Email-A	Cluster-PANEV-1	q q
July 2019	Email-A	Cluster-PANEV-1	[none given]
January 2022	Email-C	Cluster-PANEV-2	q q

16. Because the January 2022 transaction was funded with Cluster-PANEV-2, law enforcement assesses that the user who made that transaction also owns and controls Cluster-PANEV-2. That user, as explained below, was PANEV.

17. Evidence obtained in this investigation establishes that PANEV owned and controlled Email-C—the email address provided for the January 2022 transaction—at all relevant times. Specifically, and among other things, law enforcement has identified an Apple iCloud account registered to PANEV in his name bearing Email-C as the Apple ID (the "PANEV iCloud Account"). Moreover, law enforcement has obtained records for an account in PANEV's name at "Exchange-1," a major cryptocurrency exchange (the "PANEV Exchange-1 Account"). The records for the PANEV Exchange-1 Account include know-your-customer documents for PANEV, including PANEV's identification documents and personal identifying information. Those records also show that Email-C is the customer email address on the PANEV Exchange-1 Account.

18. Evidence in this investigation also establishes that PANEV owned and controlled Email-B at all relevant times. Specifically, and among other things, Email-B is listed as the verified account recovery email for Email-C based on records obtained from the provider for Email-C.

19. Based on this evidence, this investigation has shown that PANEV also owned and controlled Email-A at all relevant times. As explained above, between in or around October 2018 and in or around July 2019, Email-A was used to make transactions from Processor-1 paid for with funds from the same Bitcoin cluster—that is, Cluster-PANEV-1. In or around April 2018, Email-B was used in the same way—to make a Processor-1 payment funded by Cluster-PANEV-1. Email-A, therefore, was likely controlled by the same individual who controlled Email-B: that is, PANEV. Finally, the same user name—likely fictitious—of "q q" was provided for both the January 2022 transaction, for which Email-C (controlled by PANEV) was given, and seven of the transactions between in or around October 2018 and in or around July 2019, for which Email-A was given.

20. Therefore, this investigation has shown that PANEV initiated each of the transactions funded by Cluster-PANEV-1—that is, the first 12 of the 13 Processor-1 transactions. On at least that basis, this investigation has further shown that PANEV owned and controlled Cluster-PANEV-1 at all relevant times,

including in or around November 2018, when PANEV used funds from Cluster-PANEV-1 to register Moniker-1 on Forum-1.

PANEV Used his Service-1 Handle from the Same IP Address as His Apple iCloud Account

21. ***Second,*** the Moniker-1 records showed that Moniker-1 would, at times between in or around April 2021 and in or around September 2021, and in private messages with other Forum-1 users, pass a particular Service-1 user handle (the "PANEV Service-1 Handle") to continue communicating with those users on Service-1 rather than on Forum-1. Service-1 is structured such that a given user handle can be used by only one user.

22. Law enforcement has obtained IP address information for the PANEV Service-1 Handle. That information shows that the PANEV Service-1 Handle was used, on multiple occasions, from the same IP addresses that also accessed the PANEV iCloud Account close in time. This overlap in IP address traffic establishes that PANEV, who controlled the PANEV iCloud Account, also controlled the PANEV Service-1 Handle. And by extension, PANEV's control of the PANEV Service-1 Handle further demonstrates that PANEV also controlled Moniker-1.

23. Examples of overlapping IP address access by the PANEV Service-1 Handle and the PANEV iCloud Account follow below:

IP Address	Approximate Date and Time of Use by PANEV Service-1 Handle	Approximate Date and Time of Access by PANEV iCloud Account
[...].104	8/29/2021; 8:30 UTC	8/29/2021; 8:36 UTC
[...].1	9/8/2021; 8:20 UTC	9/8/2021; 8:23 UTC
[...].210	10/13/2021; 7:10 UTC	10/13/2021; 6:56 UTC

PANEV Received Regular Payments from LockBit Through Mixing Services

24. This investigation has also revealed that between at least as early as in or around June 2022 through at least as recently as in or around February 2024, PANEV received approximately $230,000 in regular payments of Bitcoin from a Bitcoin cluster likely controlled by one or more LockBit developers. Those payments, moreover, were laundered through multiple cryptocurrency mixing services before reaching PANEV.

25. Specifically, law enforcement has identified, with the aid of blockchain analysis software, a particular cluster of Bitcoin addresses assessed to be controlled by LockBit developers, including Khoroshev ("Cluster-LockBit"). Based on blockchain analysis, victim reports, and other investigation, law enforcement has learned that on at least two separate occasions, Cluster-LockBit

received the 20 percent developer portion of ransoms paid by LockBit victims: first, in or around October 2021, from a victim based in Utah, and second, in or around November 2021, from a victim based in New Jersey.

26. By way of background, a cryptocurrency mixing service is a service that intermingles cryptocurrency funds transferred from a sender with other funds before then transferring those funds to the intended recipient, in order to obscure the transfer directly from the sender to the recipient. Mixing services are intended and used to launder criminal proceeds and evade detection by law enforcement of the flows of funds within criminal organizations.

27. One technique used by mixing services is to receive incoming Bitcoin and leave the funds at seemingly random and disassociated addresses on the blockchain, and then transfer that same amount of Bitcoin (less transaction fees) to the ultimate recipient from a seemingly unrelated address elsewhere on the blockchain. This technique makes it difficult for anyone reviewing the publicly available blockchain to follow transfers of funds through mixing services directly from sender to recipient.

28. Another technique used by mixing services is to delay the transfer of funds to the recipient by hours, and at times even longer, again for the purpose of laundering the funds and evading detection by law enforcement.

29. Mixing services charge a fee to complete transfers by removing a small percentage of incoming funds before completing the transfer to the recipient. For this reason, when transactions conducted through a mixing service are reviewed on the blockchain, the amount reaching the final recipient is typically marginally less than the amount originally transferred from the sender.

30. A review of both the publicly available Bitcoin blockchain and the records for the PANEV Exchange-1 Account show that PANEV has received at least approximately $230,000 in Bitcoin transfers from at least as early as in or around June 2022 through at least as recently as in or around February 2024. Blockchain analysis reveals that these transfers occurred close in time to transfers from Cluster-LockBit in amounts that, although slightly larger than what was ultimately transferred to PANEV Exchange-1 Account, are virtually identical. Those slight differences are likely attributable to the fee charged by the mixing services for conducting the transactions.

31. More particularly, law enforcement has determined the following based on this evidence regarding the pattern of transfers:

a. Between at least as early as in or around June 2022 through at least as recently as in or around February 2024, Cluster-LockBit would transfer a roughly fixed amount of Bitcoin at regular intervals to some other address. Between in or around June 2022 and in or around June

2023, this amount would be roughly $5,000 in Bitcoin (based on the exchange rate at the time of the transaction) transferred every two weeks; beginning in or around July 2023 through at least as recently as in or around February 2024, this amount would be roughly $10,000 in Bitcoin (based on the exchange rate at the time) transferred once per month.

b. In at least one instance during the period from June 2022 to February 2024, blockchain analysis shows that this transfer was made to a Bitcoin address known by law enforcement to be controlled by a mixing service. In other instances, however, the funds would be transferred to an unknown and seemingly random Bitcoin address and left there—which is consistent with the operation of a mixing service.

c. On roughly the same schedule, the PANEV Exchange-1 Account would receive an incoming transfer of Bitcoin virtually identical, and close in time (sometimes even hours), to the corresponding outgoing transfer from Cluster-LockBit. Those funds would originate shortly before the final transfer to the PANEV Exchange-1 Account at one or more different Bitcoin addresses before being transferred to the PANEV Exchange-1 Account. Those intermediate Bitcoin addresses would be unknown and seemingly random—which is consistent with the operation of a mixing service.

32. The examples below illustrate this pattern. As these examples illustrate, outbound transfers from Cluster-LockBit were virtually identical in amount, and close in time, to inbound transfers to the PANEV Exchange-1 Account:

Approximate Date and Time	Approximate Outgoing Transfers from Cluster-LockBit	Approximate Date and Time	Approximate Incoming Transfers to PANEV Exchange-1 Account
6/15/2022; 9:55 UTC	0.23810532 BTC	6/15/2022; 21:31 UTC	0.23606914 BTC
7/1/2022; 14:48 UTC	0.25972395 BTC	7/1/2022; 19:13 UTC	0.25732055 BTC
9/1/2022; 15:13 UTC	0.25419 BTC	9/1/2022; 21:12 UTC	0.251877 BTC
11/30/2022; 22:42 UTC	0.29205 BTC	12/1/2022; 10:21 UTC	0.289503 BTC
4/1/2023; 15:07 UTC	0.1768 BTC	4/2/2023; 9:30 UTC	0.174832 BTC
5/15/2023; 19:55 UTC	0.18247 BTC	5/16/2023; 6:12 UTC	0.180759 BTC
12/1/2023; 12:32 UTC	0.26216 BTC	12/1/2023; 19:35 UTC	0.259592 BTC
2/1/2024; 13:06 UTC	0.23751 BTC	2/1/2024; 17:56 UTC	0.235039 BTC

33. Notably, the incoming transfers into the PANEV Exchange-1 Account of this category—that is, incoming transfers that align with outgoing transfers from Cluster-LockBit—constitute the vast majority of all incoming transfers into the PANEV Exchange-1 Account. More specifically, law enforcement has identified approximately 30 transfers into the PANEV Exchange-1 Account aligning with outgoing transfers from Cluster-LockBit; based on the Exchange-1 records, the PANEV Exchange-1 Account received only approximately 11 other incoming transfers not of that type.

34. Based on this evidence and analysis, law enforcement assesses that this pattern of Bitcoin transfers, both outgoing from Cluster-LockBit and incoming to the PANEV Exchange-1 Account, is consistent with the use of mixing services. This investigation has shown, therefore, that PANEV has received regular and significant payments of Bitcoin from the LockBit group, laundered through mixing services. Based on this investigation, including a review of the Forum-1 messages described above, there is probable cause to believe that these payments acted as compensation for development services provided by PANEV to the LockBit group.